アルゴリズム論特論　(塩田)

2015 年 6 月 1 日

宿題 反復二乗法を実装することにより、下記の素数 p たちについて、フェルマの小定理

$$2^{p-1} \equiv 1 \pmod{p}$$

を確かめてみよ。

(1) $p = 607$ (10-bit)

(2) $p = 552259$ (20-bit)

(3) $p = 900949267$ (30-bit)

(4) $p = 660768960311$ (40-bit)

(5) $p = 661425977735249$ (50-bit)

(数字はホームページからコピペした方が確かかも。)

発展課題 フェルマ・テスト、またはミラー・ラビン・テストを実装して 512 ビット程度の素数を作ってみよ。

提出期限：6 月 8 日　(メールでも紙媒体でも可)